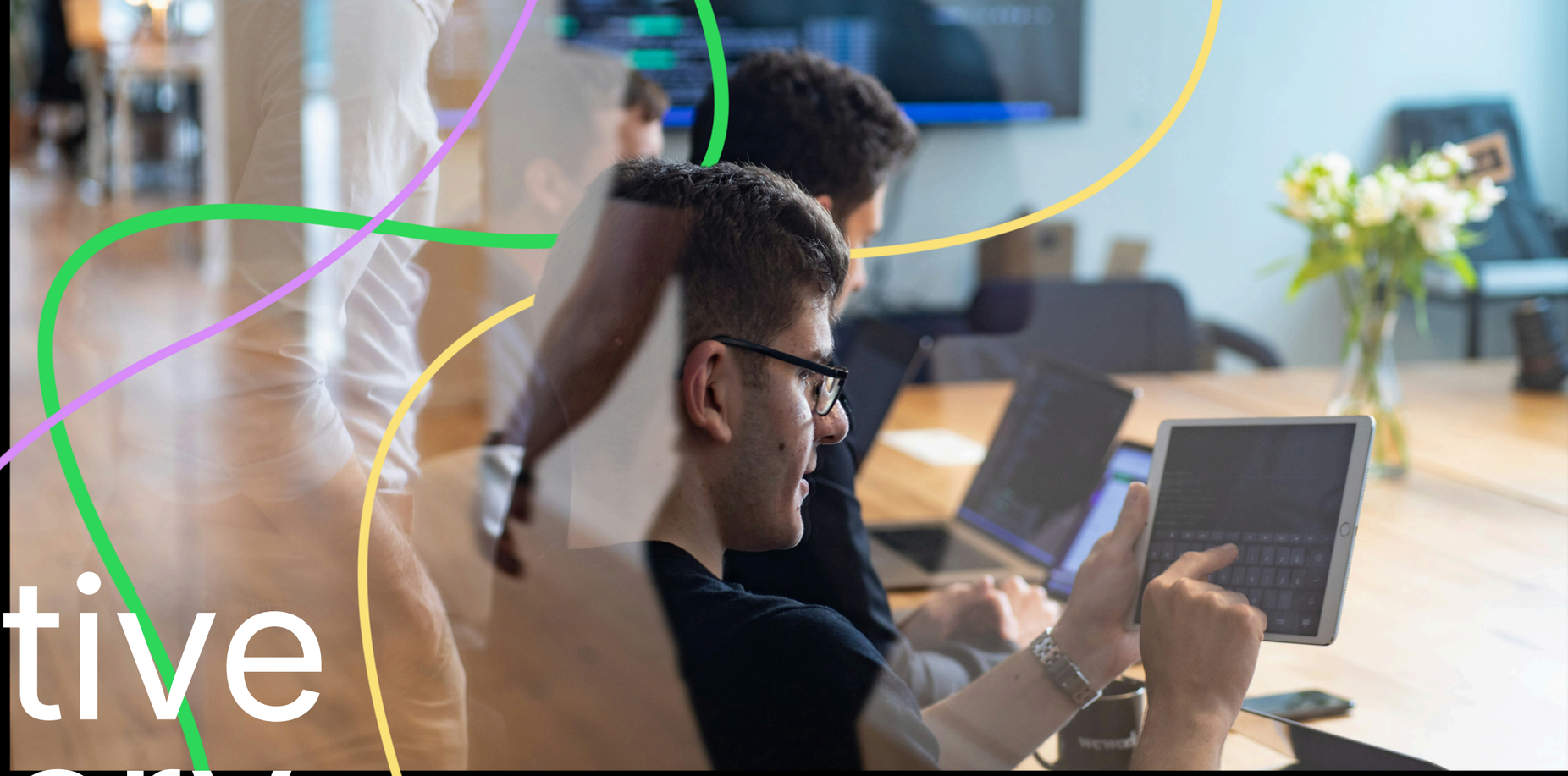
wire

The State of Secure Collaboration 2026



Why collaboration confidence is outpacing collaboration control

All statistics and findings presented in this report are derived from a Wire survey. The underlying raw data supporting these results is available upon request for verification and review purposes.



Executive summary

Core Thesis

“Organizations feel secure. Sensitive information does not stay that way. The gap is not a failure of intent; it is a structural gap between the tools available and the reality of how sensitive work actually happens.”

Most organizations believe their collaboration environments are secure. This report shows why that confidence deserves a closer look.

Wire commissioned an independent survey of 208 IT, security and compliance leaders across Germany, France and the United Kingdom. The findings reveal a persistent gap between how secure organizations believe their collaboration to be, and how sensitive information actually moves through their tools, partners and workflows.

The risk is not that organizations have ignored collaboration security. Most have policies, tools and confidence in place. The risk is that the everyday reality of collaboration, external partners, fragmented tools, shared file links, consumer messaging apps and ungoverned workflows, creates blind spots that policies alone cannot close.

Key findings

84%

Rate their collaboration environment as secure (4–5 out of 5)

48%

Say sensitive information is sometimes or often shared via tools not designed for secure communication

88%

Share sensitive information via non-secure tools at least rarely — only 12% say this never happens

81%

Say more than a quarter of sensitive collaboration involves external participants

75%

Use email as their primary method of external collaboration — only 28% use dedicated secure tools externally

42%

Use WhatsApp, Signal or similar consumer messaging apps for work collaboration

39%

Say parts of collaboration workflows are not covered by official tools — reaching 44% in the UK

82%

Are already consolidating or replacing collaboration tools, or actively searching for alternatives

Strong Sovereignty Signal

75% of respondents rate control over data location as important or very important. In Germany, this rises to 51% rating it "very important", the strongest sovereignty signal in the survey. Only 29% of respondents say their current tools are "fully suitable" for sensitive communication.

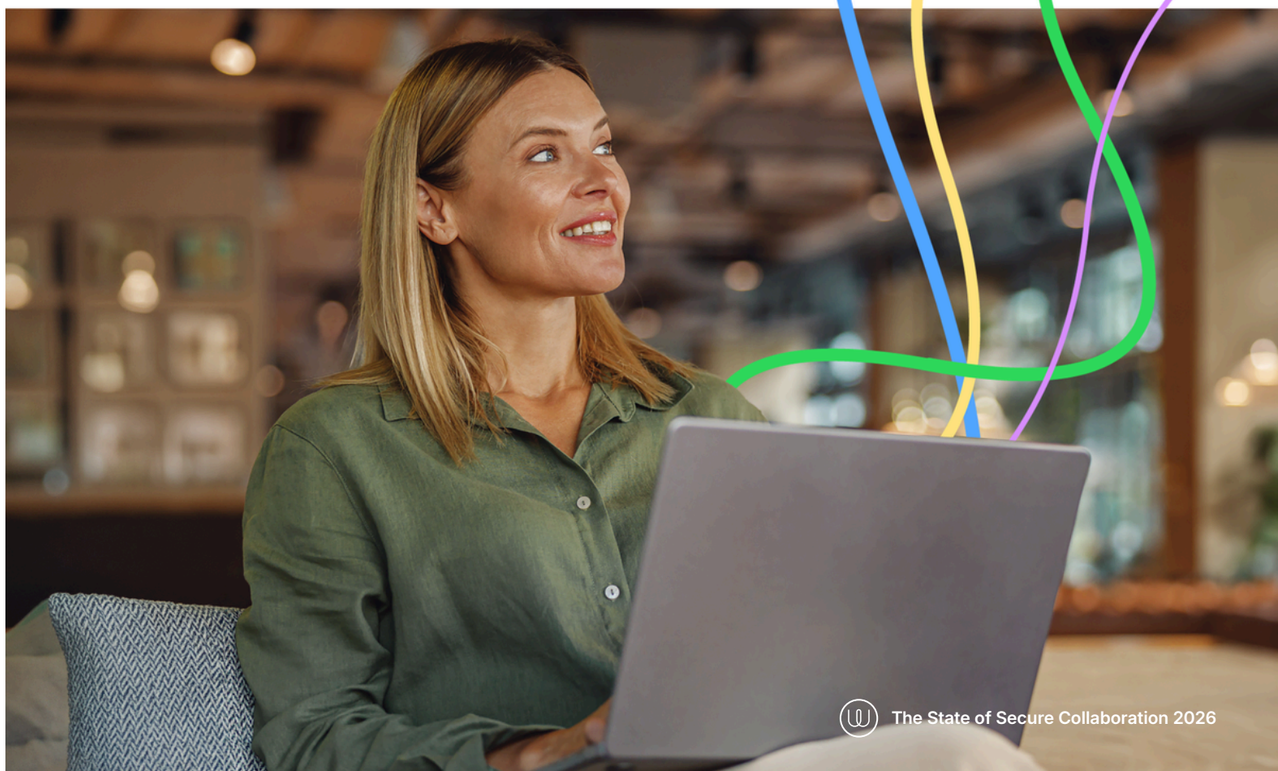
The evidence points to four structural risk areas:

1. **External collaboration:** governance breaks down fastest when sensitive work crosses organizational boundaries
2. **Consumer and unsanctioned tools:** employees turn to faster, more familiar alternatives when official tools create friction or exclude partners
3. **Compliance readiness:** confidence in regulatory preparedness does not always translate into demonstrable, auditable control
4. **Data sovereignty:** knowing where data is hosted is not the same as controlling how it moves

What this means for leaders

For IT and security leaders, the implication is not that current tools have failed. It is that mainstream collaboration tools were not designed for the control, auditability and governance that sensitive workflows require, especially where external participants are involved.

Sensitive information moves through email, file links, messaging apps and partially governed workflows daily; 45% of respondents say a collaboration-related breach would have high or critical impact, yet everyday practices still cannot reliably show who accessed what, where data is hosted, or whether external sharing was governed.



01

Why secure collaboration matters now



Collaboration has become the core operational layer of the modern organization. It is where strategic plans are drafted, financial decisions are discussed, legal documents are reviewed and sensitive client relationships are managed.
It is also where some of the most significant and least visible security risks now reside.

Three forces are driving the urgency of this issue.

Rising regulatory pressure

NIS2, DORA, GDPR and sectorspecific requirements are increasing expectations around access control, resilience, accountability and third-party risk. The survey suggests that many organizations feel prepared, but everyday collaboration practices may not fully support that confidence. 62% feel prepared or very prepared for secure collaboration requirements such as NIS2 and DORA, but 39% report workflows not covered by official tools, 61% say access remains active longer than intended at least sometimes and 48% say sensitive information is sometimes or often shared through non-secure tools.

This does not mean organizations are non-compliant. It means collaboration security is becoming a proof issue. Policies and approved tools are no longer enough if sensitive information still moves through workflows that are not fully governed.

Collaboration platforms now carry business-critical data

The shift to remote and hybrid working permanently changed what moves through collaboration tools. Messaging platforms, video calls, shared files and external workspaces now carry content that would once have been discussed only in physical meetings or managed through tightly controlled channels.

The survey confirms this directly: respondents classify financial data (76%), personal data (75%), legal and contractual documents (63%), strategic plans (53%) and operational communications (51%) as sensitive. For a significant share of organizations, all internal communication is considered sensitive.

External research reinforces the point. Forrester's 2025 data security research shows that sensitive data now extends beyond regulated records to include employee communications, cloud conversations, files, credentials, source code, AI models and unstructured data. It also identifies employee communications as one of the most commonly compromised types of corporate data across regions.
[1]

The threat environment has intensified

Collaboration platforms have become exposed to credential theft, social engineering, data exfiltration and misuse of trusted access. AI-assisted attacks are lowering the cost and increasing the sophistication of phishing, impersonation and business email compromise. Supply chain attacks and third-party access have made the perimeter of organizational data harder to define and defend.

CrowdStrike's 2026 Global Threat Report adds useful context: attackers are increasingly exploiting legitimate credentials, trusted identity flows and SaaS integrations, while many detections are malware-free. For collaboration security, this is important.

The risk is no longer only a malicious file or suspicious link. It is also a normal-looking activity inside trusted systems.

External collaboration increases the pressure further. Forrester research links part of enterprise breach exposure to attacks or incidents involving the external ecosystem, including suppliers and business partners. Secure communications research also shows that partner and supplychain communication is a priority for many leaders.

The result is an environment where the value of what passes through collaboration tools has increased significantly, while the complexity of governing those tools has grown in proportion.
[2]

Three forces are making collaboration security a 2026 priority

44%

Share of North American organizations where employee communications were the most common compromised data type
[3]

89%

Year-on-year increase in attacks by AIenabled adversaries
[4]

62%

Feel prepared for NIS2/DORA, yet 48% still share sensitive info via non-secure tools

02

The current state of collabroation

Organizations are not collaborating on one platform. They are operating across fragmented, multi-tool environments where governance is structurally difficult, even when policies are in place.



A fragmented stack

The survey shows that the typical organization uses a combination of enterprise messaging, email, video conferencing, cloud storage and consumer messaging, often simultaneously and without clear segmentation by information sensitivity or workflow type.

Collaboration Tool	% Using
Microsoft Teams	80%
Email	63%
Zoom	47%
Google Meet	44%
Whatsapp / Signal / consumer messaging apps	42%
Google Drive / Workspace	39%
SharePoint / OneDrive	18%
Dropbox	25%

Microsoft Teams dominates at 80%, but its presence does not mean collaboration is consolidated or governed. Email remains a primary tool for 63% of respondents, showing that modern collaboration stacks still depend heavily on older, less controllable infrastructure. Consumer messaging apps used by 42% of respondents confirm that tools built for personal use are now embedded in enterprise workflows.

External research supports this broader market direction: collaboration platforms are becoming central work environments, not just meeting or messaging tools. But as collaboration becomes more central, fragmented tool use becomes harder to govern.

External collaboration uses the same mixed stack

The governance challenge becomes sharper when collaboration crosses organizational boundaries. The survey shows that external collaboration still depends heavily on general-purpose channels: 75% use email with external partners or clients, 45% use file-sharing links and 42% use messaging apps. Only 28% use dedicated secure collaboration tools externally.

This matters because external participants may not follow the same policies, use the same systems or retain information in the same way. Once files and conversations move into partner environments, access control, auditability and revocation become harder.

The market is not stable

The current collaboration stack is not settled. The survey shows that 82% of organizations are either already consolidating or replacing collaboration tools, or are actively searching for alternatives. Only 15% report no plans to change.

What this means

A tool-dominant environment is not the same as a governed environment. When sensitive work moves across Teams, email, WhatsApp and shared file links (without consistent access control or audit trails) the collaboration stack is as only as strong as its weakest link.

82%

Are already consolidating or replacing tools, or still searching for alternatives

The consolidation intent is strongest among the largest organizations. Among respondents from organizations with 5,000 or more employees, 92% are already consolidating or actively searching, compared to 76% among those with 50–249 employees. For larger organizations, the collaboration stack is not just a productivity question. It is a governance and risk question.

This openness to change represents both a risk and an opportunity. Companies reassessing their collaboration stack have a genuine chance to evaluate tools not just for features and cost, but for security, governance and control, criteria that may not have been primary considerations in previous procurement decisions.



03

The security gap: Confidence vs. Reality



The central finding of this report is not that organizations are careless about collaboration security. It is that confidence in collaboration security and the reality of how sensitive information is handled exist in significant tension.

84%

Feel confident their collaboration environment is secure

79%

Are confident they control how collaboration data is accessed and shared

48%

Say sensitive information is sometimes or often shared via non-secure tools

29%

Rate their tools as “fully suitable” for sensitive communication

This gap reflects a real challenge. Security leaders are often confident in their policies, approved tools and governance frameworks, while everyday collaboration behavior continues to create exposure that those frameworks do not fully capture.

This gap is easier to understand in the context of how collaboration now works. As shown in the previous chapter, sensitive work moves across enterprise platforms, email, file links, messaging apps and external participants. In that environment, confidence in the overall collaboration environment does not always mean control over every sensitive workflow.

The suitability question is particularly instructive. While 84% feel their collaboration environment is secure, only 29% say their current tools are fully suitable for sensitive communication. This suggests that many organizations recognize a gap between the tools they use for everyday collaboration and the controls they need for sensitive work. In practice, organizations may feel broadly secure while still accepting tool limitations as a normal part of the operating environment.

The confidence gap is sharpest in the UK. UK respondents are the most likely to rate their collaboration environment as “very secure”: 47% give a score of 5 out of 5, compared to 33% in France and 24% in Germany. Yet the UK also reports the highest share of workflows not covered by official tools, at 44%. The market with the highest stated confidence also shows the most structural coverage gaps. For organizations marketing or operating in the UK, this is a meaningful signal: high confidence does not always mean fewer blind spots — it may mean they are harder to see.

That is a risk. If tools are only partially suitable for sensitive communication, then the organization may rely too heavily on policy, user judgment or manual workarounds to protect information that should be controlled by design.

Access control: a structural weakness

Beyond tool suitability, the survey reveals a persistent weakness in access governance: the ability to know who has access to shared files, and to revoke that access when it is no longer appropriate.

The business consequence is direct: 1 in 9 respondents (11%) say a collaboration-related breach would have a Critical impact on their organization. This is not a tail risk. It is a realistic exposure scenario for a meaningful share of the organizations in this survey.

When shared files retain active access long after their intended purpose, the collaboration environment accumulates risk over time. A former employee, a past contractor or an expired external partner link may retain access to sensitive content, not through a breach, but through the normal behavior of tools that do not enforce lifecycle governance.

This matters especially in a threat environment where attackers increasingly exploit trusted access and normal-looking activity. If access is no longer current, but still active, it becomes a control weakness.

What this means

This means that secure collaboration is not only about what information is shared, but also about who can still access it over time. The findings highlight a gap between confidence and control, showing that approved tools and policies are only effective if access to sensitive information can be consistently managed, monitored and revoked when needed.

34%

Find it difficult or very difficult to identify who has access to sensitive files)

61%

Say access to shared files remains active longer than intended at least sometimes after a project ends

19%

Find it difficult or very difficult to revoke access when needed

04

Where collaboration security breaks down

The confidence-control gap does not appear in one place. It shows up in the workflows where sensitive collaboration is hardest to govern: across external participants, unofficial tools, compliance requirements and data environments where location and jurisdiction matter.



These four risks are connected. A sensitive file may be shared with an external partner by email, discussed in a messaging app, stored behind a file-sharing link and remain accessible after a project ends. Each step may feel normal. Together, they create exposure.

1. External collaboration

Of all the structural weaknesses the survey identifies, external collaboration is the most critical. It is the point where organizational boundaries dissolve, where control over data, identity and access is hardest to maintain, and where the risks of an already fragmented tool environment are amplified.

The tools used for this external collaboration reveal the governance gap directly.

Method used for external collaboration	% Using
Email	75%
Same internal tools (Teams, Slack, etc.)	64%
File-sharing links (Drive, Dropbox, WeTransfer etc.)	45%
Messaging apps (Whatsapp, Signal, etc.)	42%
Dedicated secure collaboration tools	28%

Three in four organizations primarily use email for external collaboration Nearly half use file-sharing links. 42% use messaging apps. Just 28% use dedicated secure collaboration tools for external work. The loss of control at the external boundary is measurable, not just implied. 33% of respondents say they are not fully confident they retain control over files after sharing them externally, rating their confidence at 3 or below out of 5. For a third of organizations, external file sharing is already an acknowledged control weakness.

The risk is compounded when sensitive files are shared externally. Only 23% of respondents say they primarily use secure file-sharing solutions, while 27% rely on file-sharing links, 24% on collaboration platform sharing and 19% on email attachments.

External research supports the importance of this boundary. Forrester research links part of enterprise breach exposure to attacks or incidents involving the external ecosystem, including suppliers and business partners. This reinforces the survey finding: sensitive collaboration risk increases when work crosses organizational boundaries.

81%

Say more than a quarter of their sensitive collaboration involves external participants

What this means

For IT and security leaders, the implication is clear: the governance model that applies internally does not automatically extend to external collaboration. Partners, suppliers and clients operate outside the organization's identity and access framework, but they regularly receive sensitive information through the same tools used for internal work.

2. Shadow and consumer tools

The use of unsanctioned tools, including consumer messaging apps, personal cloud storage and file-sharing services, is not primarily a behavior problem. The data shows it is a workflow problem: employees use unofficial tools because official tools do not meet their needs in specific situations.

The survey identifies the triggers for bypassing official tools:

Trigger for bypassing official tools	% Total	France	Germany	UK
Urgent situation / faster alternative needed	47%	44%	55%	51%
External partner doesn't use official tools	37%	36%	37%	41%
Official tools too complex	30%	43%	21%	35%
Lack of access to official tools	25%	20%	26%	40%
Mobile / remote work context	28%	30%	30%	25%

The reason for bypassing official tools is instructive. The primary driver is speed, followed by external partners not using official tools and restrictions in the approved environment. Lack of awareness is cited by very few respondents, confirming that this is a usability and access problem, not simply a training problem.

What this means

Shadow IT in collaboration is a signal. When employees reach for WhatsApp or a personal file share to get work done, it means official tools are creating friction at the moment sensitive information needs to move. The response should not be restriction alone. It should be providing a secure alternative that is as easy to use as the consumer tools it needs to replace.

42%

Use WhatsApp, Signal or similar consumer messaging apps for work collaboration

39%

Say parts of collaboration workflows are not covered by official tools (44% in the UK, 40% in Germany)

3. Compliance Pressure

Many organizations feel prepared for the regulatory requirements that govern their collaboration environments. The survey shows that this confidence deserves careful scrutiny.

62%

Feel prepared or very prepared for secure collaboration requirements including NIS2 and DORA

That figure sits alongside findings that complicate the picture significantly:

39%

Report workflows not covered by official tools: a structural gap in governance coverage

48%

Say sensitive information is sometimes or often shared through tools not designed for secure communication

61%

Say access remains active longer than intended at least sometimes, a potential audit and accountability risk

Only 52%

Say communication and file collaboration are managed as a unified, integrated system.

NIS2, DORA and GDPR do not require organizations simply to have collaboration tools. They increase the need to demonstrate that sensitive communication is controlled, that access is governed and auditable, that data residency is known and appropriate and that incidents can be detected and reported within defined timeframes. An environment where sensitive information regularly moves through email, file links and consumer messaging apps, with access that outlasts its intended purpose, creates compliance exposure that feels invisible until it needs to be demonstrated.

What this means

For IT and security leaders, the implication is clear: the governance model that applies internally does not automatically extend to external collaboration. Partners, suppliers and clients operate outside the organization's identity and access framework, but they regularly receive sensitive information through the same tools used for internal work.



4. Data Sovereignty and Control

Data sovereignty, the ability to determine where data is held, who can access it and under what jurisdictional conditions, has moved from a technical preference to a strategic requirement for European organizations. For this report, sovereignty is assessed through respondents' views on data location control. The survey measured where collaboration data is hosted and how important location control is, jurisdictional independence and vendor-access dimensions were not directly tested and should not be inferred from these figures alone.

75%

Rate control over data location as important or very important

28%

Do not know or are unsure where their collaboration data is hosted

The German market shows the most pronounced sovereignty concern. In Germany, 51% rate data location as "very important", compared to 34% in the UK and 33% in France. This reflects both the regulatory sensitivity of the German market and a broader corporate culture in which data sovereignty is treated as a governance priority rather than a technical preference.

For organizations using global cloud platforms for collaboration, jurisdictional access is increasingly relevant to procurement and risk decisions. Knowing where data is hosted is a necessary first step; being able to demonstrate operational control over that data under the relevant legal framework is the next.

What this means

Data sovereignty in collaboration is not solely about where servers are located. It is about whether organizations can demonstrate, to regulators, clients and boards, that sensitive information remains within defined legal and jurisdictional boundaries, and that access to that information is controlled and auditable. For regulated industries and public-sector organizations, this has become a procurement threshold.

05

What secure collaboration should look like in 2026



The previous chapters show a clear pattern: organizations are not lacking collaboration tools. They are lacking consistent control over sensitive collaboration. Secure collaboration in 2026 is not defined by a single tool or a single technology, and organizations should not add more friction, more platforms or more policies so that users work around. Secure collaboration in 2026 should mean creating an environment where sensitive work can move quickly, but with the right controls built in.

The goal in 2026 is to make secure collaboration practical enough to become the default.

A maturity model for secure collaboration

Organizations can assess where they currently sit across four levels of secure collaboration maturity.

Level	Description	What this looks like in practice
1 - Ad-hoc	Collaboration happens across disconnected tools with limited control	Email, file links, and consumer apps in everyday use for sensitive work. No consistent governance. Access control is informal.
2 - Managed	Official tools exist, but control and external collaboration remain inconsistent	Enterprise tools for internal work, but email and consumer apps still dominate external collaboration. Policies exist but coverage is incomplete.
3 - Controlled	Access, governance and compliance needs are recognized and increasingly managed	Segmented tools for different sensitivity levels. Access control policies applied. Compliance alignment in progress. External collaboration partially governed.
4 - Secure by Design	Collaboration is secure by design, governed consistently and ready for sensitive, external and regulated use cases	End-to-end governance across internal and external workflows. Full access lifecycle control. Auditable, sovereign, demonstrably compliant.

The survey data places most organizations in the Managed-to-Controlled range. 39% report collaboration workflows not covered by official tools, and only 52% say communication and file collaboration are managed as a fully integrated system, both indicators of incomplete governance coverage. At the same time, 48% say sensitive information is sometimes or often shared through tools not designed for secure communication, and 61% say access to shared files remains active longer than intended. Organizations in this range have built the policy and tool foundation. What they have not yet closed is the loop between policy, workflow and demonstrable control.

What the secure collaboration layer must deliver

For organizations handling sensitive, regulated or externally facing work, six capabilities are becoming essential.

Controlled messaging and file collaboration
Sensitive content should stay within a governed environment instead of spreading across inboxes, file links, downloads and personal devices.

Secure external access
Partners, suppliers, clients and contractors should be brought into controlled spaces with defined, limited and revocable access, rather than defaulting to email or consumer apps.

Access lifecycle management
Organizations need visibility into who has access to sensitive files and the ability to revoke access when the work is complete.

Data location control
Leaders should be able to define and verify where collaboration data is hosted, and demonstrate that to regulators, clients and boards.

Audit readiness
Communication and file-sharing records should support compliance reporting, incident investigation and regulatory response.

Resilient crisis communication
Organizations need a secure channel for leadership and operational teams when primary systems are unavailable, compromised or no longer trusted.

The role of AI in future secure collaboration

The next evolution of collaboration risk is not limited to humans sharing files and messages. AI tools are becoming part of the collaboration environment as meeting transcription services, writing assistants, workflow automation agents and integration layers. Each of these creates new questions about where sensitive content is processed, stored and accessed. Market research identified AI agents as emerging “personas” inside collaboration environments, with their own access rights, data processing footprints and integration points. In addition AI-enabled adversaries, identity abuse, SaaS flows and malware-free attacks are mankind trusted collaboration environments more exposed.

06

Practical recommendations

The following recommendations can help organizations move toward secure-by-design collaboration.

1. Define what sensitive collaboration means

Turn data classification into practical collaboration rules.

Define which information and workflows require stronger control, including legal reviews, financial discussions, client work, strategic planning, incident response and external partner exchanges. Make clear which tools are approved for each type of sensitive work.

2. Map where sensitive work actually happens

Look beyond approved tools.

Map where sensitive conversations, files and decisions move across email, messaging apps, file links, shared drives, collaboration platforms and external partners. Identify where policy and practice do not match.

3. Treat external collaboration as its own security domain

Do not assume internal controls extend to partners, suppliers and clients.

Create specific rules for external collaboration, including controlled guest access, limited permissions, revocable file sharing, time-bound access, audit trails and clear offboarding when work ends.

4. Make the secure path easier than the workaround

Shadow tools are often a sign that official workflows are too slow, restrictive or difficult to use.

Identify where employees bypass approved tools and remove the friction. Provide secure alternatives that are fast enough for urgent work and simple enough for external participants to use.

5. Manage access across the full file lifecycle

Do not treat sharing as the end of the control process.

Set ownership, expiry dates and review points for sensitive files and workspaces. Regularly audit who has access, remove outdated permissions and close external access when projects or relationships end.

6. Build compliance evidence into collaboration workflows

Policies are not enough if control cannot be demonstrated.

Ensure collaboration tools and processes can show who accessed what, when access changed, where data was hosted, how information was shared and when access was revoked.

7. Make data sovereignty part of procurement

Evaluate collaboration tools not only on features and cost, but also on data location, jurisdictional access, deployment options, administration rights, encryption and auditability.

For sensitive or regulated workflows, assess whether sovereign, private or hybrid deployment models are needed.

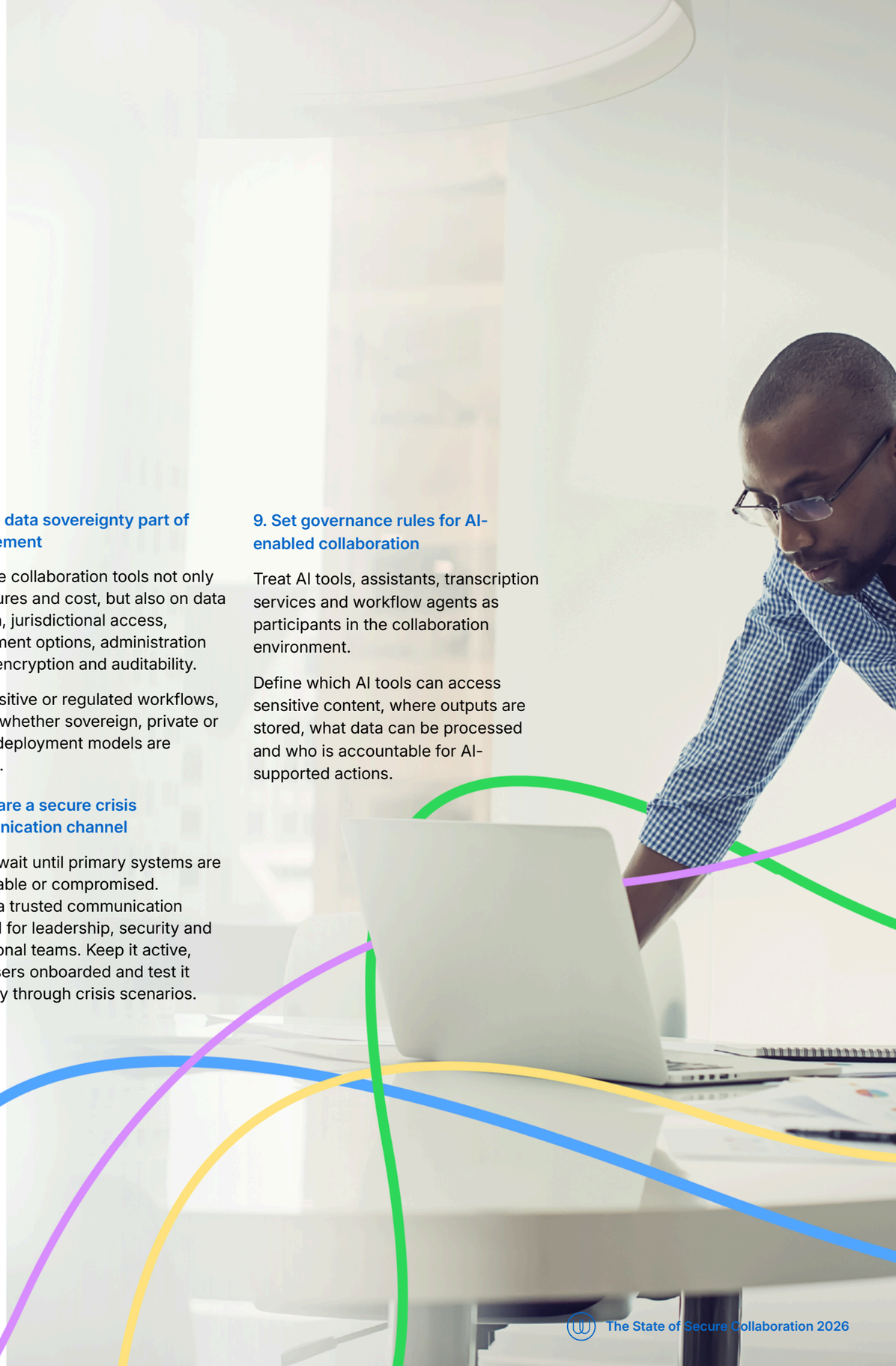
8. Prepare a secure crisis communication channel

Do not wait until primary systems are unavailable or compromised. Define a trusted communication channel for leadership, security and operational teams. Keep it active, keep users onboarded and test it regularly through crisis scenarios.

9. Set governance rules for AI-enabled collaboration

Treat AI tools, assistants, transcription services and workflow agents as participants in the collaboration environment.

Define which AI tools can access sensitive content, where outputs are stored, what data can be processed and who is accountable for AI-supported actions.



07

Modern collaboration with security at its core

Meet Wire's user-friendly platform designed to outmaneuver evolving threats and meet strict regulations.

Government-Grade Security
BSI VS-NfD certified and the only collaboration platform approved for classified use in Germany, with security standards equivalent to NATO Confidential.

Regulatory-Ready Compliance
Fully compliant with GDPR and NIS2, and certified to ISO 27001, ISO 27701, and UK Cyber Essentials standards.

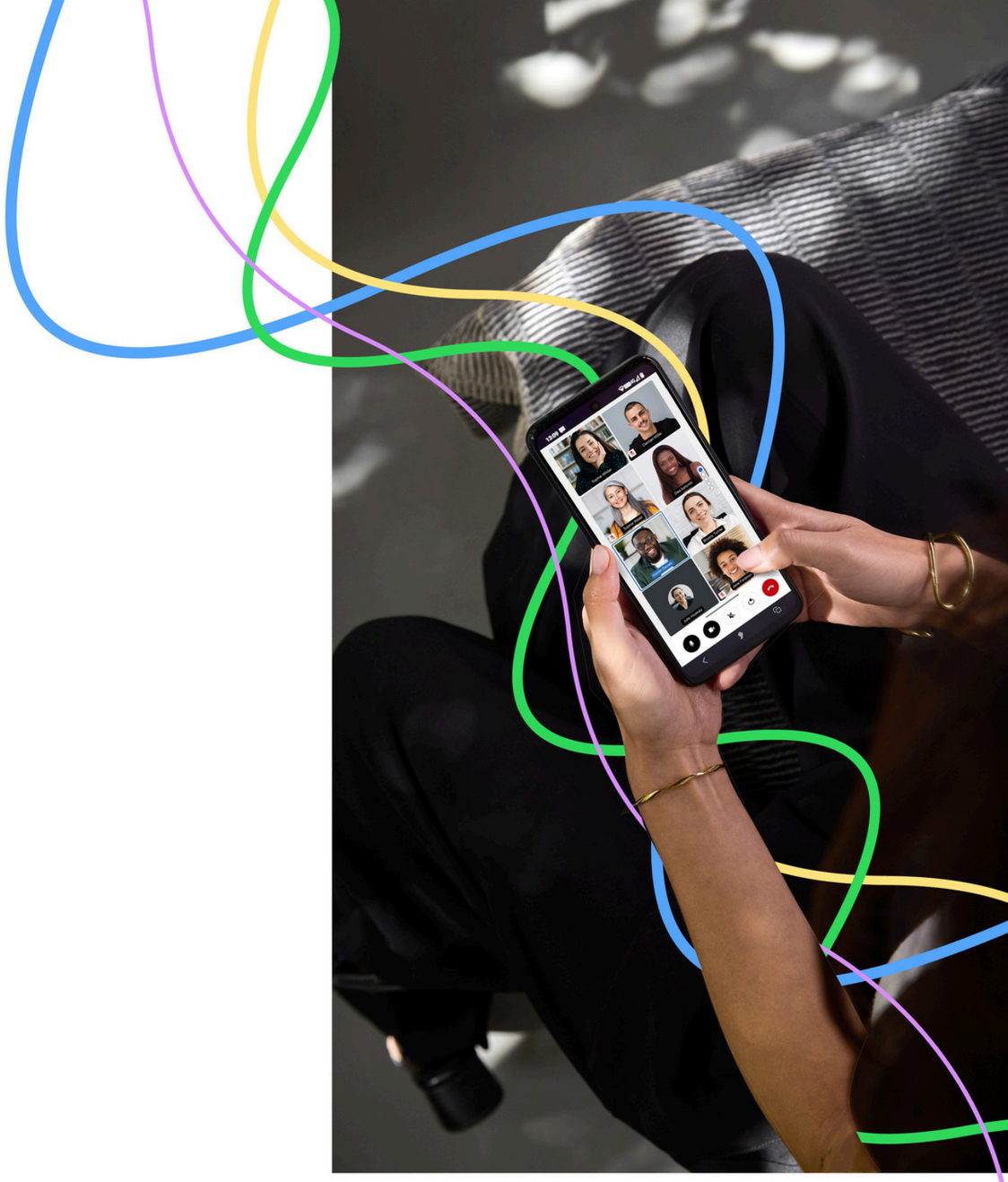
All-in-One Collaboration
Secure messaging, voice and video calling, conferencing, and file sharing in a single platform, accessible from any device.

Seamless User Experience
Enterprise-grade security built in, with support for apps, browsers, and up to 8 devices per user without impacting performance.

Next-Generation Encryption
The industry's only full Messaging Layer Security (MLS) implementation, providing post-quantum-ready protection for all communications, including voice and video calls.

wire.com

CLICK HERE TO BOOK A DEMO



08

Methodology

Wire commissioned an independent survey of 208 IT, security, and compliance decision-makers across Germany, France, and the United Kingdom.

The survey was conducted in Q3 2025. Respondents represent organisations of varying sizes — from small and medium-sized enterprises to large corporations — across sectors including technology, financial services, critical infrastructure, defence, and the public sector.

The data presented in this report reflects respondents' answers. Statistically robust country comparisons and size segmentations were made where sample sizes (n ≥ 40) permit. Industry splits are available for Technology & Software (n=92), Financial Services (n=42), and Critical Infrastructure / Defence / Public Sector (combined, n=46).

[1]
Market validation: Forrester State of Data Security 2025, cited in Market Research Insights.

[2]
Source: CrowdStrike 2026 Global Threat Report; Forrester State of Data Security 2025; Forrester/Element Future of Secure Communications, cited in Market Research Insights

[3]
(Forrester 2025)

[4]
(CrowdStrike 2026)

© 2026 Wire Swiss GmbH. All rights reserved. This report was produced on the basis of an independent survey. All statistics are based on Wire primary research unless otherwise stated.